UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/087,000	02/28/2002	Penny C. Leavy	10009.000110	6351

7590 02/21/2006

Arnold M. de Guzman
De Guzman and carpenter LLP
5276 Hollister Avenue
Suite 160
Santa Barbara, CA 93111

EXAMINER	
GUYTON, PHILIP A	

ART UNIT	PAPER NUMBER
2113	

DATE MAILED: 02/21/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 10/087,000	**Applicant(s)** LEAVY ET AL.	
	Examiner Philip Guyton	**Art Unit** 2113	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 February 2002*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5,7,8,17,19,24,25,27 and 28* is/are rejected.

7)☒ Claim(s) *6,9-16,18,20-23 and 26* is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *28 February 2002* is/are: a)□ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

Drawings

1. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they do not include the following reference signs mentioned in the description: 805a, 810a, and 815a on page 35; 905 and 910 on page 36; 1015 on page 38.

2. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(4) because reference character 910 has been used to designate both "delimiter" on page 36 of the specification and "fault" in figure 9.

Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Specification

3. The disclosure is objected to because of the following informalities:

Reference to "patterns 200" on page 7, line 19 should be "patterns 210."

Reference to “input fields 500 in a transaction 505” should be “input fields 505 in a transaction 500.”

Reference to “figure 1200” on page 65, line 1 should be “figure 12.”

Appropriate correction is required.

Claim Rejections - 35 USC § 101

4. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claim 2 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The claim is directed towards “a machine-readable medium” which, when taken as broad as reasonably possible, include embodiments which are not a process, machine, manufacture, or composition of matter as required by 35 U.S.C. 101. For example, a program code written on paper is a machine-readable medium, but is clearly non-statutory subject matter under 35 U.S.C. 101. It is suggested that machine-readable medium be substituted with computer-readable medium.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

6. Claims 1-5, 7, 8, 17, 24, 25, 27, and 28 are rejected under 35 U.S.C. 102(a) as being anticipated by "Insertion, Evasion, and Denial of Server; Eluding Network Intrusion Detection" by Ptacek et al. (Ptacek).

With respect to claim 1, Ptacek discloses a method of creating a fault-inducing transaction representation in a network (page 2, abstract), the method comprising:

interjecting a pattern with fault-inducing sub-fields (page 11, section 3.1, paragraphs 1-2 – *"An IDS can…past an IDS."*), where the pattern is an expression including a literal string and a wildcard character class (page 11, section 3.1, paragraphs 3-4 – *"To understand…data it observes."*); and

using the expression to form a subsequent expression that can be used by a target system to detect and trigger on the network at least one transaction that matches the expression (pages 5-6, section 1.3, paragraphs 1-4 – *"The question of…of an attack."*).

Claim 2 is an article of manufacture for performing the method of claim 1, and is rejected under the same rationale.

Claim 3 is an apparatus for performing the method of claim 1, and is rejected under the same rationale.

With respect to claim 4, Ptacek discloses a method of testing a target in a network by fault injection (page 2, abstract), the method comprising:

defining a transaction baseline (page 44, section 7.1, paragraph 6 – *"Before conducting…reproduction string."*);

modifying at least one of an order and a structure of the transaction baseline to obtain a modified transaction with malformed grammar (pages 10-11, section 3, paragraphs 1-2 – *"We discuss…past the analyzer."*); and

transmitting the modified transaction to a target (page 45, section 7.3, paragraph 1 – *"Each of our tests…to the target host."*).

With respect to claim 5, Ptacek discloses after transmitting the modified transaction, receiving feedback from the target to determine fault occurrence (page 44, section 7.1, paragraph 3 – *"In addition…the subject IDS."*).

With respect to claim 7, Ptacek discloses wherein the modifying step comprises removing a field from the transaction (pages 12-13, section 3.2, paragraph 4 – *"In the insertion…most ID systems."*).

With respect to claim 8, Ptacek discloses wherein the modifying step comprises duplicating a field in the transaction (page 47, operation frag-4).

With respect to claim 17, Ptacek discloses wherein the modifying step comprises using value injection to alter an input field in the transaction (page 11, section 3.1, paragraphs 3-4 – *"To understand…data it observes."*).

With respect to claim 24, Ptacek discloses a method of testing a target on a network by fault injection (page 2, abstract), the method comprising:

defining a transaction baseline (page 44, section 7.1, paragraph 6 – *"Before conducting…reproduction string."*);

modifying an input field in the transaction baseline to obtain a modified transaction with malformed value (page 46, operation frag-3); and transmitting the modified transaction to a target (page 45, section 7.3, paragraph 1 – *"Each of our tests…to the target host."*).

With respect to claim 25, Ptacek discloses after transmitting the modified transaction, receiving a feedback from the target to determine fault occurrence (page 44, section 7.1, paragraph 3 – *"In addition…the subject IDS."*).

With respect to claim 27, Ptacek discloses a method of testing a target in a network by fault injection (page 2, abstract), the method comprising:

defining a transaction baseline (page 44, section 7.1, paragraph 6 – *"Before conducting…reproduction string."*);

modifying the transaction baseline to obtain modified transaction with an extraneous metacharacter (page 47, operation frag-5); and

transmitting the modified transaction to a target (page 45, section 7.3, paragraph 1 – *"Each of our tests…to the target host."*).

With respect to claim 28, Ptacek discloses an apparatus for testing a target in a network by fault injection (page 2, abstract), the apparatus comprising:

a driver configured to generate patterns, where pattern can generate a plurality of packets for transmission to the target (page 45, section 7.3, paragraph 1 – *"Each of our…to the target host."*), the pattern being represented by an expression with a literal string and a wild character class (page 11, section 3.1, paragraphs 3-4 – *"To understand…data it observes."*); and

a network interface coupled to the driver and configured to transmit and receive network traffic (page 45, section 7.2, paragraph 5 – *"Our test network…our tests."*).

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

8. Claims 1-5, 7, 17, 19, 24, 25, 27, and 28 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 6,584,569 to Reshef et al. (Reshef).

With respect to claim 1, Reshef discloses a method of creating a fault-inducing transaction representation in a network (abstract), the method comprising:

interjecting a pattern with fault-inducing sub-fields (column 3, line 60-column 4, line 8), where the pattern is an expression including a literal string and a wildcard character class (column 10, table 1 – ie. change parameter value, append to path, etc); and

using the expression to form a subsequent expression that can be used by a target system to detect and trigger on the network at least one transaction that matches the expression (column 10, lines 25-35).

Claim 2 is an article of manufacture for performing the method of claim 1, and is rejected under the same rationale.

Claim 3 is an apparatus for performing the method of claim 1, and is rejected under the same rationale.

With respect to claim 4, Reshef discloses a method of testing a target in a network by fault injection (abstract), the method comprising:

defining a transaction baseline (column 10, lines 25-31);

modifying at least one of an order and a structure of the transaction baseline to obtain a modified transaction with malformed grammar (column 10, lines 31-35 and table 1); and

transmitting the modified transaction to a target (figure 3C, step 314).

With respect to claim 5, Reshef discloses after transmitting the modified transaction, receiving feedback from the target to determine fault occurrence (figure 3C, step 316).

With respect to claim 7, Reshef discloses wherein the modifying step comprises removing a field from the transaction (column 10, table 1 – change parameter value to null).

With respect to claim 17, Reshef discloses wherein the modifying step comprises using value injection to alter an input field in the transaction (column 10, table 1 – change value).

With respect to claim 19, Reshef discloses wherein the modifying step comprises determining a value injection based on numerical ranges of the input field content (column 10, table 1 – increase string length beyond maxlength).

With respect to claim 24, Reshef discloses a method of testing a target on a network by fault injection (abstract), the method comprising:

defining a transaction baseline (column 10, lines 25-31);

modifying an input field in the transaction baseline to obtain a modified transaction with malformed value (column 10, lines 31-35 and table 1); and

transmitting the modified transaction to a target (figure 3C, step 316).

With respect to claim 25, Reshef discloses after transmitting the modified transaction, receiving a feedback from the target to determine fault occurrence (figure 3C, step 316).

With respect to claim 27, Reshef discloses a method of testing a target in a network by fault injection (abstract), the method comprising:

defining a transaction baseline (column 10, lines 25-31);

modifying the transaction baseline to obtain modified transaction with an extraneous metacharacter (column 10, table 1 – increase string length beyond maxlength); and

transmitting the modified transaction to a target (figure 3C, step 316).

With respect to claim 28, Reshef discloses an apparatus for testing a target in a network by fault injection (abstract), the apparatus comprising:

a driver configured to generate patterns, where pattern can generate a plurality of packets for transmission to the target (column 5, lines 16-20), the pattern being represented by an expression with a literal string and a wild character class (column 10, table 1 – ie. change parameter value, append to path, etc); and

a network interface coupled to the driver and configured to transmit and receive network traffic (figure 2A, item 14 and column 4, line 61-column 5, line 7).

Allowable Subject Matter

9. Claims 6, 9-16, 18, 20-23, and 26 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

10. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See PTO-892.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Philip Guyton whose telephone number is (571) 272-3807. The examiner can normally be reached on M-F 8:00-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Robert Beausoliel can be reached on (571) 272-3645. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

PG
2/14/06

[illegible]
[illegible]
[illegible]